What is claimed is:

1. An apparatus for use in encryption or decryption, for solving a system of linear equations $Ax=b$ in n unknowns on a finite field $GF(p)$, where p is a prime, n is a positive integer, A is a coefficient matrix consisting of elements of n rows and n columns, x is a vector of unknowns consisting of n elements, and b is a constant vector consisting of n elements, the apparatus comprising:

parameter storing means for storing the coefficient matrix A and the constant vector b;

triangular transforming means for reading the coefficient matrix A and the constant vector b from the parameter storing means, and transforming the read coefficient matrix A and constant vector b to generate a coefficient matrix C and a constant vector d for a system of linear equations $Cx=d$ in n unknowns that is equivalent to the system of linear equations $Ax=b$, the coefficient matrix C consisting of elements of n rows and n columns and the constant vector d consisting of n elements, wherein the coefficient matrix A is triangular transformed into the coefficient matrix C of upper triangular form without diagonal elements of the coefficient matrix A being changed to 1;

diagonal element inverting means for calculating inverses of diagonal elements of the generated coefficient matrix C on the

finite field *GF(p)*; and

equation computing means for solving the system of linear equations *Cx=d* using the coefficient matrix *C*, the constant vector *d*, and the inverses of the diagonal elements of the coefficient matrix *C*, to thereby solve the system of linear equations *Ax=b*.

2. The apparatus of Claim 1,

wherein the triangular transforming means performs one or more successive transformation processes to generate the coefficient matrix *C* and the constant vector *d* of the system of linear equations *Cx=d* from the coefficient matrix *A* and the constant vector *b* of the system of linear equations *Ax=b*,

wherein in each transformation process the triangular transforming means transforms a coefficient matrix and a constant vector of a system of linear equations in *n* unknowns, into a coefficient matrix and a constant vector of a system of linear equations in *n* unknowns that is equivalent to the system of linear equations before the transformation, where the system of linear equations *Ax=b* is subjected to the first transformation process and the system of linear equations *Cx=d* is generated as a result of the last transformation process,

wherein in each transformation process the system of linear equations in *n* unknowns that is subjected to the transformation

includes one pivotal equation which is a linear equation serving as a pivot for the transformation and one or more object equations which are linear equations to be transformed, and the triangular transforming means transforms each of the object equations into an equation equivalent to the object equation by

defining a first coefficient group containing at least one value related to the pivotal equation and a second coefficient group containing *n+1* values related to the pivotal equation,

changing a nonzero coefficient in the object equation to *0*, and

multiplying each of a constant and *n* coefficients in the object equation by the value in the first coefficient group, and subtracting the *n+1* values in the second coefficient group respectively from the *n+1* multiplication results.

3. The apparatus of Claim 2,

wherein each transformation process has transformation subprocesses each for transforming a separate one of the object equations,

wherein in each transformation subprocess the triangular transforming means

(a) chooses a nonzero coefficient from the pivotal equation and sets the chosen nonzero coefficient into the first coefficient group,

(b) chooses a nonzero coefficient from the object equation, multiplies each of a constant and *n* coefficients in the pivotal equation by the nonzero coefficient chosen from the object equation, and sets *n+1* values obtained by the multiplications into the second coefficient group,

(c) changes the chosen nonzero coefficient in the object equation to *0*, and

(d) multiplies each of a constant and *n* coefficients in the object equation by the nonzero coefficient in the first coefficient group, and subtracts the *n+1* values in the second coefficient group respectively from the *n+1* multiplication results.

4. The apparatus of Claim 3,

wherein when the diagonal elements of the coefficient matrix *C* are denoted by m_i *(i=1,2,...,n)* and the inverses of the diagonal elements m_i *(i=1,2,...,n)* in the finite field *GF(p)* are denoted by I_i *(i=1,2,...,n)*, the diagonal element inverting means includes

(a) a multiplying unit for computing

$$t_i = \prod_{k=1}^{n} m_k \ (\text{except } m_i) \ mod\ p \ (i=1,2,...,n)$$

and

$$t = \prod_{k=1}^{n} m_k \ mod\ p$$

(b) a first inverting unit for computing

$$u=1/t \bmod p$$

and

(c) a second inverting unit for computing

$$I_i=u\times t_i \bmod p \quad (i=1,2,\ldots,n)$$

to find the inverses I_i $(i=1,2,\ldots,n)$.

5. The apparatus of Claim 4,

wherein the multiplying unit calculates

$$s_1=m_1\times m_2 \bmod p$$

$$s_2=s_1\times m_3 \bmod p$$

$$\vdots$$

$$s_{n-3}=s_{n-4}\times m_{n-2} \bmod p$$

in the stated order, then calculates

$$t_n=s_{n-3}\times m_{n-1} \bmod p$$

$$t_{n-1}=s_{n-3}\times m_n \bmod p$$

$$s_n=m_{n-1}\times m_n \bmod p$$

$$t_{n-2}=s_{n-4}\times s_n \bmod p$$

$$s_{n-1}=m_{n-2}\times s_n \bmod p$$

$$t_{n-3}=s_{n-5}\times s_{n-1} \bmod p$$

$$s_{n-2}=m_{n-3}\times s_{n-1} \bmod p$$

$$t_{n-4}=s_{n-6}\times s_{n-2} \bmod p$$

$$\vdots$$

$$s_5=m_4\times s_6 \bmod p$$

$t_3=s_1 \times s_5 \bmod p$

$s_4=m_3 \times s_5 \bmod p$

$t_2=m_1 \times s_4 \bmod p$

$t_1=m_2 \times s_4 \bmod p$

in the stated order, and lastly calculates

$t=t_j \times m_j$

for a value j chosen from a set of positive integers $\{1,2,\ldots,n\}$.

6. The apparatus of Claim 2,

wherein each transformation process has a coefficient group calculation process and transformation subprocesses, performed following the coefficient group calculation process, each for transforming a separate one of the object equations,

wherein in the coefficient group calculation process the triangular transforming means

(a) chooses m nonzero coefficients by taking one nonzero coefficient from each of the pivotal equation and the object equations, multiplies each combination of $(m-1)$ of the chosen nonzero coefficients, and sets the m multiplication results into the first coefficient group, m being a positive integer no smaller than 2, and

(b) multiplies each of a constant and n coefficients in the pivotal equation by a multiplication result in the first

coefficient group for a combination of nonzero coefficients that does not include a nonzero coefficient chosen from the pivotal equation, and sets *n+1* values obtained by the multiplications into the second coefficient group, and

wherein in each of the transformation subprocesses following the coefficient group calculation process, the triangular transforming means

(a) changes a nonzero coefficient chosen from the object equation in the coefficient group calculation process, to *0* in the object equation, and

(b) multiplies each of a constant and *n* coefficients in the object equation by a multiplication result in the first coefficient group for a combination of nonzero coefficients that does not include the nonzero coefficient chosen from the object equation, and subtracts the *n+1* values in the second coefficient group respectively from the *n+1* multiplication results.

7. The apparatus of Claim 6,

wherein when the diagonal elements of the coefficient matrix *C* are denoted by m_i *(i=1,2,...,n)* and the inverses of the diagonal elements m_i *(i=1,2,...,n)* in the finite field *GF(p)* are denoted by I_i *(i=1,2,...,n)*, the diagonal element inverting means includes

(a) a multiplying unit for computing

$$t_i = \prod_{k=1}^{n} m_k \text{ (except } m_i) \bmod p \quad (i=1,2,\ldots,n)$$

and

$$t = \prod_{k=1}^{n} m_k \bmod p$$

(b) a first inverting unit for computing

$$u = 1/t \bmod p$$

and

(c) a second inverting unit for computing

$$I_i = u \times t_i \bmod p \quad (i=1,2,\ldots,n)$$

to find the inverses I_i $(i=1,2,\ldots,n)$.

8. The apparatus of Claim 7,

wherein the multiplying unit calculates

$$s_1 = m_1 \times m_2 \bmod p$$

$$s_2 = s_1 \times m_3 \bmod p$$

$$\vdots$$

$$s_{n-3} = s_{n-4} \times m_{n-2} \bmod p$$

in the stated order, then calculates

$$t_n = s_{n-3} \times m_{n-1} \bmod p$$

$$t_{n-1} = s_{n-3} \times m_n \bmod p$$

$$s_n = m_{n-1} \times m_n \bmod p$$

$$t_{n-2} = s_{n-4} \times s_n \bmod p$$

$$s_{n-1} = m_{n-2} \times s_n \bmod p$$

$$t_{n-3}=s_{n-5}\times s_{n-1} \bmod p$$

$$s_{n-2}=m_{n-3}\times s_{n-1} \bmod p$$

$$t_{n-4}=s_{n-6}\times s_{n-2} \bmod p$$

$$\vdots$$

$$s_5=m_4\times s_6 \bmod p$$

$$t_3=s_1\times s_5 \bmod p$$

$$s_4=m_3\times s_5 \bmod p$$

$$t_2=m_1\times s_4 \bmod p$$

$$t_1=m_2\times s_4 \bmod p$$

in the stated order, and lastly calculates

$$t=t_j\times m_j$$

for a value j chosen from a set of positive integers $\{1,2,\ldots,n\}$.

9. An apparatus for use in encryption or decryption, for computing an inverse I of an element y in $GF(q)$ which is an extension field of a finite field $GF(p)$, where p is a prime, $q=p^n$, and n is a positive integer, the apparatus comprising:

equation generating means for generating a coefficient matrix A and a constant vector b for a system of linear equations $Ax=b$ in n unknowns, using the element y and all coefficients of a generator polynomial of $GF(q)$ whose root is α;

equation solving means for finding solutions of the system of linear equations $Ax=b$, the equation solving means including

the apparatus of Claim 1; and

inverse computing means for computing the inverse I using the root α and the solutions found by the equation solving means.

10. An apparatus for use in encryption or decryption, for computing an inverse I of an element y in $GF(q)$ which is an extension field of a finite field $GF(p)$, where p is a prime, $q=p^n$, and n is a positive integer, the apparatus comprising:

equation generating means for generating a coefficient matrix A and a constant vector b for a system of linear equations $Ax=b$ in n unknowns, using the element y and all coefficients of a generator polynomial of $GF(q)$ whose root is α;

equation solving means for finding solutions of the system of linear equations $Ax=b$, the equation solving means including the apparatus of Claim 2; and

inverse computing means for computing the inverse I using the root α and the solutions found by the equation solving means.

11. An apparatus for use in encryption or decryption, for computing an inverse I of an element y in $GF(q)$ which is an extension field of a finite field $GF(p)$, where p is a prime, $q=p^n$, and n is a positive integer, the apparatus comprising:

equation generating means for generating a coefficient matrix A and a constant vector b for a system of linear equations $Ax=b$

in n unknowns, using the element y and all coefficients of a generator polynomial of $GF(q)$ whose root is α;

equation solving means for finding solutions of the system of linear equations $Ax=b$, the equation solving means including the apparatus of Claim 3; and

inverse computing means for computing the inverse I using the root α and the solutions found by the equation solving means.

12. An apparatus for use in encryption or decryption, for computing an inverse I of an element y in $GF(q)$ which is an extension field of a finite field $GF(p)$, where p is a prime, $q=p^n$, and n is a positive integer, the apparatus comprising:

equation generating means for generating a coefficient matrix A and a constant vector b for a system of linear equations $Ax=b$ in n unknowns, using the element y and all coefficients of a generator polynomial of $GF(q)$ whose root is α;

equation solving means for finding solutions of the system of linear equations $Ax=b$, the equation solving means including the apparatus of Claim 4; and

inverse computing means for computing the inverse I using the root α and the solutions found by the equation solving means.

13. An apparatus for use in encryption or decryption, for computing an inverse I of an element y in $GF(q)$ which is an

extension field of a finite field $GF(p)$, where p is a prime, $q=p^n$, and n is a positive integer, the apparatus comprising:

equation generating means for generating a coefficient matrix A and a constant vector b for a system of linear equations $Ax=b$ in n unknowns, using the element y and all coefficients of a generator polynomial of $GF(q)$ whose root is α;

equation solving means for finding solutions of the system of linear equations $Ax=b$, the equation solving means including the apparatus of Claim 5; and

inverse computing means for computing the inverse I using the root α and the solutions found by the equation solving means.

14. An apparatus for use in encryption or decryption, for computing an inverse I of an element y in $GF(q)$ which is an extension field of a finite field $GF(p)$, where p is a prime, $q=p^n$, and n is a positive integer, the apparatus comprising:

equation generating means for generating a coefficient matrix A and a constant vector b for a system of linear equations $Ax=b$ in n unknowns, using the element y and all coefficients of a generator polynomial of $GF(q)$ whose root is α;

equation solving means for finding solutions of the system of linear equations $Ax=b$, the equation solving means including the apparatus of Claim 6; and

inverse computing means for computing the inverse I using the

root α and the solutions found by the equation solving means.

15. An apparatus for use in encryption or decryption, for computing an inverse I of an element y in $GF(q)$ which is an extension field of a finite field $GF(p)$, where p is a prime, $q=p^n$, and n is a positive integer, the apparatus comprising:

equation generating means for generating a coefficient matrix A and a constant vector b for a system of linear equations $Ax=b$ in n unknowns, using the element y and all coefficients of a generator polynomial of $GF(q)$ whose root is α;

equation solving means for finding solutions of the system of linear equations $Ax=b$, the equation solving means including the apparatus of Claim 7; and

inverse computing means for computing the inverse I using the root α and the solutions found by the equation solving means.

16. An apparatus for use in encryption or decryption, for computing an inverse I of an element y in $GF(q)$ which is an extension field of a finite field $GF(p)$, where p is a prime, $q=p^n$, and n is a positive integer, the apparatus comprising:

equation generating means for generating a coefficient matrix A and a constant vector b for a system of linear equations $Ax=b$ in n unknowns, using the element y and all coefficients of a generator polynomial of $GF(q)$ whose root is α;

equation solving means for finding solutions of the system of linear equations $Ax=b$, the equation solving means including the apparatus of Claim 8; and

inverse computing means for computing the inverse I using the root α and the solutions found by the equation solving means.

17. A record medium reproducing apparatus for computing, when copyrighted digital content has been encrypted using a discrete logarithm problem on an elliptic curve E over $GF(q)$ as a basis for security and recorded on a record medium, an inverse I of an element y in $GF(q)$ to decrypt the encrypted digital content recorded on the record medium, where $GF(q)$ is an extension field of a finite field $GF(p)$, p is a prime, $q=p^n$, n is a positive integer, and G is a base point of the elliptic curve E, the record medium reproducing apparatus comprising:

equation generating means for generating a coefficient matrix A and a constant vector b for a system of linear equations $Ax=b$ in n unknowns, using the element y and all coefficients of a generator polynomial of $GF(q)$ whose root is α;

equation solving means for finding solutions of the system of linear equations $Ax=b$, the equation solving means including the apparatus of Claim 1; and

inverse computing means for computing the inverse I using the root α and the solutions found by the equation solving means.

18. A record medium reproducing apparatus for computing, when copyrighted digital content has been encrypted using a discrete logarithm problem on an elliptic curve E over $GF(q)$ as a basis for security and recorded on a record medium, an inverse I of an element y in $GF(q)$ to decrypt the encrypted digital content recorded on the record medium, where $GF(q)$ is an extension field of a finite field $GF(p)$, p is a prime, $q=p^n$, n is a positive integer, and G is a base point of the elliptic curve E, the record medium reproducing apparatus comprising:

equation generating means for generating a coefficient matrix A and a constant vector b for a system of linear equations $Ax=b$ in n unknowns, using the element y and all coefficients of a generator polynomial of $GF(q)$ whose root is α;

equation solving means for finding solutions of the system of linear equations $Ax=b$, the equation solving means including the apparatus of Claim 2; and

inverse computing means for computing the inverse I using the root α and the solutions found by the equation solving means.

19. A record medium reproducing apparatus for computing, when copyrighted digital content has been encrypted using a discrete logarithm problem on an elliptic curve E over $GF(q)$ as a basis for security and recorded on a record medium, an inverse I of an

element y in $GF(q)$ to decrypt the encrypted digital content recorded on the record medium, where $GF(q)$ is an extension field of a finite field $GF(p)$, p is a prime, $q=p^n$, n is a positive integer, and G is a base point of the elliptic curve E, the record medium reproducing apparatus comprising:

equation generating means for generating a coefficient matrix A and a constant vector b for a system of linear equations $Ax=b$ in n unknowns, using the element y and all coefficients of a generator polynomial of $GF(q)$ whose root is α;

equation solving means for finding solutions of the system of linear equations $Ax=b$, the equation solving means including the apparatus of Claim 3; and

inverse computing means for computing the inverse I using the root α and the solutions found by the equation solving means.

20. A record medium reproducing apparatus for computing, when copyrighted digital content has been encrypted using a discrete logarithm problem on an elliptic curve E over $GF(q)$ as a basis for security and recorded on a record medium, an inverse I of an element y in $GF(q)$ to decrypt the encrypted digital content recorded on the record medium, where $GF(q)$ is an extension field of a finite field $GF(p)$, p is a prime, $q=p^n$, n is a positive integer, and G is a base point of the elliptic curve E, the record medium reproducing apparatus comprising:

equation generating means for generating a coefficient matrix A and a constant vector b for a system of linear equations $Ax=b$ in n unknowns, using the element y and all coefficients of a generator polynomial of $GF(q)$ whose root is α;

equation solving means for finding solutions of the system of linear equations $Ax=b$, the equation solving means including the apparatus of Claim 4; and

inverse computing means for computing the inverse I using the root α and the solutions found by the equation solving means.

21. A record medium reproducing apparatus for computing, when copyrighted digital content has been encrypted using a discrete logarithm problem on an elliptic curve E over $GF(q)$ as a basis for security and recorded on a record medium, an inverse I of an element y in $GF(q)$ to decrypt the encrypted digital content recorded on the record medium, where $GF(q)$ is an extension field of a finite field $GF(p)$, p is a prime, $q=p^n$, n is a positive integer, and G is a base point of the elliptic curve E, the record medium reproducing apparatus comprising:

equation generating means for generating a coefficient matrix A and a constant vector b for a system of linear equations $Ax=b$ in n unknowns, using the element y and all coefficients of a generator polynomial of $GF(q)$ whose root is α;

equation solving means for finding solutions of the system

of linear equations $Ax=b$, the equation solving means including the apparatus of Claim 5; and

inverse computing means for computing the inverse I using the root α and the solutions found by the equation solving means.

22. A record medium reproducing apparatus for computing, when copyrighted digital content has been encrypted using a discrete logarithm problem on an elliptic curve E over $GF(q)$ as a basis for security and recorded on a record medium, an inverse I of an element y in $GF(q)$ to decrypt the encrypted digital content recorded on the record medium, where $GF(q)$ is an extension field of a finite field $GF(p)$, p is a prime, $q=p^n$, n is a positive integer, and G is a base point of the elliptic curve E, the record medium reproducing apparatus comprising:

equation generating means for generating a coefficient matrix A and a constant vector b for a system of linear equations $Ax=b$ in n unknowns, using the element y and all coefficients of a generator polynomial of $GF(q)$ whose root is α;

equation solving means for finding solutions of the system of linear equations $Ax=b$, the equation solving means including the apparatus of Claim 6; and

inverse computing means for computing the inverse I using the root α and the solutions found by the equation solving means.

23. A record medium reproducing apparatus for computing, when copyrighted digital content has been encrypted using a discrete logarithm problem on an elliptic curve E over $GF(q)$ as a basis for security and recorded on a record medium, an inverse I of an element y in $GF(q)$ to decrypt the encrypted digital content recorded on the record medium, where $GF(q)$ is an extension field of a finite field $GF(p)$, p is a prime, $q=p^n$, n is a positive integer, and G is a base point of the elliptic curve E, the record medium reproducing apparatus comprising:

equation generating means for generating a coefficient matrix A and a constant vector b for a system of linear equations $Ax=b$ in n unknowns, using the element y and all coefficients of a generator polynomial of $GF(q)$ whose root is α;

equation solving means for finding solutions of the system of linear equations $Ax=b$, the equation solving means including the apparatus of Claim 7; and

inverse computing means for computing the inverse I using the root α and the solutions found by the equation solving means.

24. A record medium reproducing apparatus for computing, when copyrighted digital content has been encrypted using a discrete logarithm problem on an elliptic curve E over $GF(q)$ as a basis for security and recorded on a record medium, an inverse I of an element y in $GF(q)$ to decrypt the encrypted digital content

recorded on the record medium, where *GF(q)* is an extension field of a finite field *GF(p)*, *p* is a prime, $q=p^n$, *n* is a positive integer, and *G* is a base point of the elliptic curve *E*, the record medium reproducing apparatus comprising:

equation generating means for generating a coefficient matrix *A* and a constant vector *b* for a system of linear equations *Ax=b* in *n* unknowns, using the element *y* and all coefficients of a generator polynomial of *GF(q)* whose root is α;

equation solving means for finding solutions of the system of linear equations *Ax=b*, the equation solving means including the apparatus of Claim 8; and

inverse computing means for computing the inverse *I* using the root α and the solutions found by the equation solving means.

25. A method for solving a system of linear equations *Ax=b* in *n* unknowns on a finite field *GF(p)* where *p* is a prime, *n* is a positive integer, *A* is a coefficient matrix consisting of elements of *n* rows and *n* columns, *x* is a vector of unknowns consisting of *n* elements, and *b* is a constant vector consisting of *n* elements, for use in encryption or decryption in an apparatus equipped with parameter storing means which stores the coefficient matrix *A* and the constant vector *b*, the method comprising:

a triangular transforming step for reading the coefficient matrix *A* and the constant vector *b* from the parameter storing means, and transforming the read coefficient matrix *A* and constant vector *b* to generate a coefficient matrix *C* and a constant vector *d* for a system of linear equations *Cx=d* in *n* unknowns that is equivalent to the system of linear equations *Ax=b*, the coefficient matrix *C* consisting of elements of *n* rows and *n* columns and the constant vector *d* consisting of *n* elements, wherein the coefficient matrix *A* is triangular transformed into the coefficient matrix *C* of upper triangular form without diagonal elements of the coefficient matrix *A* being changed to *1*;

a diagonal element inverting step for calculating inverses of diagonal elements of the generated coefficient matrix *C* on the finite field *GF(p)*; and

an equation computing step for solving the system of linear equations *Cx=d* using the coefficient matrix *C*, the constant vector *d*, and the inverses of the diagonal elements of the coefficient matrix *C*, to thereby solve the system of linear equations *Ax=b*.

26. The method of Claim 25,

wherein the triangular transforming step includes one or more successive transformation processes to generate the coefficient

matrix *C* and the constant vector *d* of the system of linear equations *Cx=d* from the coefficient matrix *A* and the constant vector *b* of the system of linear equations *Ax=b*,

wherein in each transformation process a coefficient matrix and a constant vector of a system of linear equations in *n* unknowns are transformed into a coefficient matrix and a constant vector of a system of linear equations in *n* unknowns that is equivalent to the system of linear equations before the transformation, where the system of linear equations *Ax=b* is subjected to the first transformation process and the system of linear equations *Cx=d* is generated as a result of the last transformation process,

wherein in each transformation process the system of linear equations in *n* unknowns that is subjected to the transformation includes one pivotal equation which is a linear equation serving as a pivot for the transformation and one or more object equations which are linear equations to be transformed, and each of the object equations is transformed into an equation equivalent to the object equation by

defining a first coefficient group containing at least one value related to the pivotal equation and a second coefficient group containing *n+1* values related to the pivotal equation,

changing a nonzero coefficient in the object equation to *0*, and

multiplying each of a constant and *n* coefficients in the object equation by the value in the first coefficient group, and subtracting the *n+1* values in the second coefficient group respectively from the *n+1* multiplication results.

27. The method of Claim 26,

wherein each transformation process has transformation subprocesses each for transforming a separate one of the object equations,

wherein in each transformation subprocess

(a) a nonzero coefficient is chosen from the pivotal equation and set into the first coefficient group,

(b) a nonzero coefficient is chosen from the object equation, each of a constant and *n* coefficients in the pivotal equation is multiplied by the nonzero coefficient chosen from the object equation, and *n+1* values obtained by the multiplications are set into the second coefficient group,

(c) the chosen nonzero coefficient in the object equation is changed to *0*, and

(d) each of a constant and *n* coefficients in the object equation is multiplied by the nonzero coefficient in the first coefficient group, and the *n+1* values in the second coefficient group are subtracted respectively from the *n+1* multiplication results.

28. The method of Claim 27,

wherein when the diagonal elements of the coefficient matrix C are denoted by m_i $(i=1,2,...,n)$ and the inverses of the diagonal elements m_i $(i=1,2,...,n)$ in the finite field $GF(p)$ are denoted by I_i $(i=1,2,...,n)$, the diagonal element inverting step includes

(a) a multiplying substep for computing

$$t_i=\prod_{k=1}^{n} m_k \text{ (except } m_i) \bmod p \quad (i=1,2,...,n)$$

and

$$t=\prod_{k=1}^{n} m_k \bmod p$$

(b) a first inverting substep for computing

$$u=1/t \bmod p$$

and

(c) a second inverting substep for computing

$$I_i=u\times t_i \bmod p \quad (i=1,2,...,n)$$

to find the inverses I_i $(i=1,2,...,n)$.

29. The method of Claim 28,

wherein the multiplying substep calculates

$$s_1=m_1\times m_2 \bmod p$$

$$s_2=s_1\times m_3 \bmod p$$

⋮

$$s_{n-3}=s_{n-4}\times m_{n-2} \bmod p$$

in the stated order, then calculates

$$t_n=s_{n-3}\times m_{n-1} \bmod p$$

$$t_{n-1}=s_{n-3}\times m_n \bmod p$$

$$s_n=m_{n-1}\times m_n \bmod p$$

$$t_{n-2}=s_{n-4}\times s_n \bmod p$$

$$s_{n-1}=m_{n-2}\times s_n \bmod p$$

$$t_{n-3}=s_{n-5}\times s_{n-1} \bmod p$$

$$s_{n-2}=m_{n-3}\times s_{n-1} \bmod p$$

$$t_{n-4}=s_{n-6}\times s_{n-2} \bmod p$$

$$\vdots$$

$$s_5=m_4\times s_6 \bmod p$$

$$t_3=s_1\times s_5 \bmod p$$

$$s_4=m_3\times s_5 \bmod p$$

$$t_2=m_1\times s_4 \bmod p$$

$$t_1=m_2\times s_4 \bmod p$$

in the stated order, and lastly calculates

$$t=t_j\times m_j$$

for a value j chosen from a set of positive integers $\{1,2,\ldots,n\}$.

30. The method of Claim 26,

wherein each transformation process includes a coefficient group calculation process and transformation subprocesses,

performed following the coefficient group calculation process, each for transforming a separate one of the object equations,

wherein in the coefficient group calculation process

(a) *m* nonzero coefficients are chosen by taking one nonzero coefficient from each of the pivotal equation and the object equations, each combination of (*m-1*) of the chosen nonzero coefficients is multiplied, and the *m* multiplication results are set into the first coefficient group, *m* being a positive integer no smaller than *2*, and

(b) each of a constant and *n* coefficients in the pivotal equation is multiplied by a multiplication result in the first coefficient group for a combination of nonzero coefficients that does not include a nonzero coefficient chosen from the pivotal equation, and *n+1* values obtained by the multiplications are set into the second coefficient group,

wherein in each of the transformation subprocesses following the coefficient group calculation process

(a) a nonzero coefficient chosen from the object equation in the coefficient group calculation process is changed to *0* in the object equation, and

(b) each of a constant and *n* coefficients in the object equation is multiplied by a multiplication result in the first coefficient group for a combination of nonzero coefficients that does not include the nonzero coefficient chosen from the object

equation, and the $n+1$ values in the second coefficient group are subtracted respectively from the $n+1$ multiplication results.

31. The method of Claim 30,

wherein when the diagonal elements of the coefficient matrix C are denoted by m_i $(i=1,2,...,n)$ and the inverses of the diagonal elements m_i $(i=1,2,...,n)$ in the finite field $GF(p)$ are denoted by I_i $(i=1,2,...,n)$, the diagonal element inverting step includes

(a) a multiplying substep for computing

$$t_i=\prod_{k=1}^{n} m_k \text{ (except } m_i) \bmod p \ (i=1,2,...,n)$$

and

$$t=\prod_{k=1}^{n} m_k \bmod p$$

(b) a first inverting substep for computing

$$u=1/t \bmod p$$

and

(c) a second inverting substep for computing

$$I_i=u\times t_i \bmod p \ (i=1,2,...,n)$$

to find the inverses I_i $(i=1,2,...,n)$.

32. The method of Claim 31,

wherein the multiplying substep calculates

$$s_1=m_1\times m_2 \bmod p$$

$$s_2=s_1\times m_3 \bmod p$$

$$\vdots$$

$$s_{n-3}=s_{n-4}\times m_{n-2} \bmod p$$

in the stated order, then calculates

$$t_n=s_{n-3}\times m_{n-1} \bmod p$$

$$t_{n-1}=s_{n-3}\times m_n \bmod p$$

$$s_n=m_{n-1}\times m_n \bmod p$$

$$t_{n-2}=s_{n-4}\times s_n \bmod p$$

$$s_{n-1}=m_{n-2}\times s_n \bmod p$$

$$t_{n-3}=s_{n-5}\times s_{n-1} \bmod p$$

$$s_{n-2}=m_{n-3}\times s_{n-1} \bmod p$$

$$t_{n-4}=s_{n-6}\times s_{n-2} \bmod p$$

$$\vdots$$

$$s_5=m_4\times s_6 \bmod p$$

$$t_3=s_1\times s_5 \bmod p$$

$$s_4=m_3\times s_5 \bmod p$$

$$t_2=m_1\times s_4 \bmod p$$

$$t_1=m_2\times s_4 \bmod p$$

in the stated order, and lastly calculates

$$t=t_j\times m_j$$

for a value j chosen from a set of positive integers $\{1,2,\ldots,n\}$.